2020-08-03

A novel approach for improving information security management and awareness for home environments

Alotaibi, F

10.1108/ICS-05-2020-0073
Information and Computer Security
Emerald

A novel approach for improving information security management and awareness for home environments

Journal:	*Information and Computer Security*
Manuscript ID	ICS-05-2020-0073
Manuscript Type:	Original Article
Keywords:	Information security management, Information security awareness, Human factors, Home users, Information security policy

A novel approach for improving information security management and awareness for home environments

Abstract

Purpose - The human factor is a major consideration in securing systems. A wide and increasing range of different technologies, devices, platforms, applications and services are being used every day by home users. In parallel, home users are also experiencing a range of different online threats and attacks and are increasingly being targeted as they lack the knowledge and awareness about potential threats and how to protect themselves. The increase in technologies and platforms also increases the burden upon a user to understand how to apply security across the differing technologies, operating systems and applications. This results in managing the security across their technology portfolio increasingly more troublesome and time consuming. This paper aims to propose an approach that attempts to propose a system for improving security management and awareness for home users.

Design/methodology/approach - The proposed system is capable of creating and assigning different security policies for different digital devices in a user-friendly fashion. These assigned policies are monitored, checked and managed in order to review the user's compliance with the assigned policies in order to provide a bespoke awareness content based on the user's current needs.

Findings – A novel framework was proposed for improving information security management and awareness for home users. In addition, A mock-up design was developed to simulate the proposed approach to visualise the main concept and the functions which might be performed when it is deployed in a real environment. A number of different scenarios have been simulated in order to show how the system can manage and deal with different types of users, devices and threats. In addition, the proposed approach has been evaluated by experts in the research domain. The overall feedback is positive, constructive and encouraging. The experts agreed that the identified research problem is a real problem. In addition, they agreed that the proposed approach is usable, feasible and effective in improving security management and awareness for home users.

Practical implication – This study offers a framework and usable mock-up design which can help in improving information security management for home users

Research limitations/implications –The proposed design of the system is a mock-up design without real data. Therefore, implementing the proposed approach in a real environment can provide the researcher with a better understanding of the effectiveness and the functionality of the proposed approach.

Originality/value - Improving the security management and awareness for home users by monitoring, checking and managing different security controls and configurations effectively are the key to strengthen information security. Therefore, when home users have a good level of security management and awareness, this could protect and secure the home network and subsequently business infrastructure and services as well.

Keywords Information security management, Information security awareness, Human factors, home users, Information security policy

Paper type Research paper

1 Introduction

With the rapid development of information technology including smartphones, computers, tablets, smartwatches and the Internet of Things, providing security for home digital devices and services become more essential and more challenging as many home users face online threats and attacks (Nthala *et al*, 2018). According to the Office for National Statistics (National Office of Statistics, 2018), 90% of households in Great Britain had internet access in 2018 including 81% of British adults using smartphones, 63% use laptops and 57 % have tablets. Worldwide, there were around 27 billion Internet of Things (IoT) connected devices worldwide by 2019, an increase from 15 billion devices in 2014 and it is expected to reach 75.44 billion devices by 2025 (Statista, 2019). Due to this increase in internet access and devices, more online threats and malicious attacks are experienced by home users.

NCSA and PayPal (2013) conducted a study to analyse the cyber security behaviors and perceptions of home users in the United of States. The result revealed that more than half of the participants (55%) did not configure a PIN code to protect their smartphones, 14% used one password or PIN across all the online accounts and 20% never changed their passwords. In addition, less than one-quarter of the respondents (21.6%) installed security software such as antivirus. Another study was conducted by Watson and Zheng (2017) to assess the security awareness for the US mobile users. They found that around 20% of the participants did not configure any screen locking protection such as PIN or fingerprint. In addition, 20% used unofficial sources to download applications, 85% have had a virus and 80% have downloaded malicious applications.

The situation might be worse in the developing countries as evidenced by the study of Rao and Pati (2012) in India. More than 80% of respondents used torrent.com to download software, games and movies. The results show 64% of home users did not use anti-virus software, 71% claimed that they were not sure about their security settings in their browsers, 80% indicated that they had no clue about malware, worms, spyware and phishing and 78% did not know about personal firewalls. 64% did not have Anti-virus software in their systems while only 10% had a licenced antivirus software.

The common attacks and threats targeting home users are: operating systems vulnerabilities, malware, phishing, identity theft and privacy violation (Rao and Pati, 2012). Nthala *et al*, (2018) state that all these threats are usually mitigated well in large organisations because they have security policies, segmented network architectures, firewall, Antivirus, IDS, IPS, patching management, backup solutions and IT support team. In contrast, very few security resources, ability, knowledge, skills and tools are available to protect home users from a wide range of threats and attacks. The lack of appropriate awareness, monitoring and management for the security configurations could make the digital devices at homes more vulnerable and easily compromised. Therefore, they might experience security breaches which could be used to attack critical infrastructures and services such as telecommunication and banking and other organisations (Ng and Rahim, 2005). For example, X-Box Live, the PlayStation Network, Dyn (DNS provider), UK's TalkTalk and Post Office online services have been affected by a DDoS attack which was a botnet coordinated through a large number of Internet of Things (IoT) devices in homes that had been hacked and infected with malware(Lunsford and Boahn, 2015; Reynolds, 2016).

Some researchers have claimed that most of the cyber security awareness and education courses and initiatives are designed and conducted for the organisations and the business environment (Kritzinger and Von Solms, 2010). Online portals such as Get Safe online and Stay Safe Online are the most common available resources used by home users but they provide generic information and basic knowledge (Magaya and Clarke, 2012). This can make these portals not useful for beginners and novices which might not be useful for some users who have different skills or issues. they argued that some of these online portals do not have a clear structure and navigation which can make it difficult for novice users to use and find the required information. In addition, some of these portals do not provide up-to-date information and not covering all the relevant security awareness and issues (Kritzinger and Von Solms, 2010).

The above studies and events show that the home users are vulnerable and targeted by many online threats due to applying weak security practices and controls, difficulty in monitoring and managing different digital devices and lack of appropriate security awareness. Many researchers argued that security protection and practice can be improved by enhancing and promoting security awareness for home users (Furnell *et al.*, 2007; Nouh *et al.*, 2014). Therefore, an alternative approach needs to be explored which has the ability to promote and increase security awareness amongst home users by providing a bespoke security awareness in a centralised and usable manner to meet the current needs of the users.

This study proposes a comprehensive a framework for improving security management and awareness for home users. The proposed approach seeks to unify the multi-device, multi-platform and pervasive threat environment into a usable single home-user security information manager by mapping complex security requirements in an adaptable manner; being mindful of technologies, services and people. several initial interfaces were deigned and evaluated by 434 participants in our previous work (Alotaibi *et al.*, 2019). Those findings were used to develop the framework and a mock-up design was developed base to simulate the proposed framework to show different interactions with different components and sections in order to visualise the main concepts and functions which can be performed when it is deployed in a real environment. After designing the proposed framework and simulating it using the mock-up design, the framework and the mock-up design The results which paper w result research designed several preliminary interfaces which has been evaluated by conducting focus group session with experts in the cyber security domain. The interviewed experts agreed that the identified problem in the research is a real problem that needs to be investigated and solved. In addition, the overall feedback of the experts about the framework and the mock-up design was positive and satisfactory.

In this paper, the current state of the art and related works are analysed and presented in Section 2. The proposed information security management system and its mock-up design are discussed and presented in Section 3. Section 4 provides the result of the evaluation of the proposed system. Section 5 provides the concluding remarks and future works.

2 Related Works

A variety of studies which have tried to raise the security awareness of home users towards different online threats, including phishing attacks, social engineering attacks, security controls and configurations and general security. Some of these studies have tried to provide home users with cyber security awareness which are tailored to their needs in different aspects. A limited number of studies have tried to assess home users' security knowledge, restrict their online activity and force them to access awareness materials if

they do not have sufficient knowledge (Kritzinger and Von Solms, 2010; Labuschagne and Eloff, 2012; Alotaibi *et al.*, 2017). Kritzinger and Von Solms (2010) have tried to provide an appropriate awareness content based on the level of security knowledge for the users. They proposed a theoretical E-Awareness Model (E-AM) which can provide awareness topics and materials based on the knowledge level of home users. The user must be tested in order to be assigned to the appropriate level of the three levels: novice, intermediate and advanced. However, they suggested that Internet Services Providers (ISPs) should host and handle the proposed tool in order to enforce home users to access awareness content. Two years later, Kritzinger and Von Solms (2013) suggested theoretically a technical approach that can move the technical security protection responsibility (firewall, strong password, anti-virus, updates, patches) from home users to ISPs. Labuschagne and Eloff (2012) proposed a security awareness system by using a virtualized system on shared computers instead of being hosted by ISPs. The system assesses users' security knowledge and allows them accessing the internet if their level of security knowledge is satisfactory. Supposing that ISPs will take the responsibility of providing security management and awareness for home users, this can make an extra effort and tasks by monitoring, managing and configuring with different technical controls and settings with multiple devices connecting via different ISPs. Moreover, an additional financial cost has to be paid by home users for providing this service. In addition, this type of restricted enforcement might annoy and disturb the users' online activity. Additionally, this type of intervention from ISPs might make some privacy issues because ISPs will store and deal with confidential information for home users and their devices which can be breached and exposed which put home users at risk and start blaming ISPs for any issues which might happen for their devices and information. These issues might lead them to reject this approach or try to bypass the portal.

Another tool was introduced by Magaya and Clarke (2012) to provide a bespoke recommendation and guideline by assessing the online behavior of home users and identifying and prioritizing the missing security controls from high to low. However, the process of detecting the controls and service currently implemented is done in a manual way from the user side which could be difficult for some novice users. Moreover, the tool does not have the ability to check the effectiveness of each implemented control. For instance, if the user selects that the password is configured, the tool will exclude it from the missing control list without identifying the password strength which might be weak.

Several studies were focused in enhancing the security awareness of phishing attacks (Jahankhani *et al.*, 2011; Maurer *et al.*, 2011; Sharifi *et al.*, 2011; Volkamer *et al.*, 2015). They proposed approaches and tools are intended to work as a browser extension and provide a bespoke awareness for users about phishing websites and the possible threats while surfing online. While other researchers proposed methods to raise security awareness about different online threats by developing awareness web portals (Tolnai and Von Solms, 2009; Smith *et al.*, 2013). However, these portals do not have the ability to provide bespoke awareness content which can promote security awareness.

An analysis of these studies has revealed that most studies have made efforts in proposing "one-fits-all" solutions that do not have the ability to provide the users with a tailored awareness content based on some criteria such as the current needs, prior knowledge, and security priorities for each user. This review indicates that there is a need for an approach that can provide the users with bespoke awareness information which can enhance the security practice among home users as evidenced by some studies (LaRose, Rifon and Enbody, 2008; Davinson and Sillence, 2010). In addition, Ho*we et al* (2012) argued that there is current need to integrate all the security activities and configurations in a comprehensive tool which can improve security and reduce the heavy load on home users in managing different security tools and settings for different threats. Another recent study was conducted by Nthala *et al.* (2018) revealed that there is a clear need to develop a usable

convenient tool can be used by non-experts to manage the security configurations for different devices and services at home which could motivate home users for better security and simplify the task for them. In the same context, Rao and Pati (2012) identified in their study that there is a current need to develop a usable tool for awareness and security controls management based on users' knowledge and behavioural pattern which could improve home users' perception of information security.

Therefore, it is clear that there is a need for a bespoke individualized personalized approach that takes into account knowledge and awareness of the technologies, applications, and services that users use and provides bespoke information directly based upon the current security posture. In order to measure and understand how the home users are doing something (i.e. well or badly), it needs to be defined against something – in an organisation, this would be a security policy. Despite the fact that many approaches and tools have been proposed for the home users to promote cybersecurity, they are providing general, static and limited awareness content. Therefore, there is a need to propose an approach which has the ability to monitor and manage the security practice for home users by applying some form of security policies in order to deliver customized awareness content and encourage the users to practice better security, similar to the approach which has already implemented in organisations.

3 The proposed information security management and awareness system

Despite the fact that the above analysis of the literature review shows that many approaches and tools have been proposed for the home users to promote cybersecurity, they are providing general, static and limited awareness content. In addition, the above events and studies show that home users suffer from different issues such as lack of security knowledge, lack of understanding of the security concepts, the lack of willingness to manage and monitor different security settings across different devices. In addition, there is a lack of providing a tailored security awareness based on the users' needs. These leaves users open to a variety of attacks that would compromise their information, systems and networks.

Accordingly, it is clear that there is a need for a usable, educational bespoke individualized approach which can configure, manage and monitor information security across devices and technologies and services within the home. In the approach, it is suggested as part of the solution is to use and apply different security policies in order to measure and understand how home users are managing and controlling their security. The following requirements need to be considered and addressed in the proposed architecture in order to offer an effective security management system:

- **Security policies and levels:** different groups of security policies are required to be defined and assigned for devices and users. The policies should cover different operating systems and technologies including their security configuration, settings and controls which can enhance their protection and security once being configured and managed effectively. The security policies can be configured and defined based on three levels: low, medium and high. This can provide good flexibility and granularity in the proposed system in order to meet the users' needs. For instance, the low level can contain the minimum requirements which need to be configured in the devices and it can be assigned for novice users who do not have good technology experience.
- **Usable interfaces:** the components of the system interfaces should be easy to access, use and understand in order to help the system to achieve its main objectives and goals. The interfaces need to be designed based on HCI and usability principles in order to meet the users' requirements and satisfaction.

- **Automatic recognition sensor:** the system should have an automatic recognition feature which can allow it to scan, identify and recognise new digital devices which have not been enrolled in the system yet in order to be added. The system should have the ability to assign an appropriate security policy for the devices.
- **Automatic security check:** the proposed system should review continuously the configured security settings and controls on the managed devices in order to be compared with the assigned policies in order to check the security compliance.
- **The enrolment process:** the novice users should be given an almost automatic configuration process where is a little to nothing for them to have to do, including baseline security measure is used to provide A level of protection for them.
- **Security Concern and Knowledge:** the system should have the ability to raise security concerns and knowledge in order to raise and improve security management as it is evident by the results of the questionnaire.
- **A tailored security awareness content:** the proposed system should be able to deliver tailored security awareness customised based on the users' knowledge and their current needs. This will help to deal effectively with different types of users who have different levels of knowledge and requirements.
- **A comprehensive profile:** The system should have the ability to provide the users (administrator and end-user) with a comprehensive profile in a usable method which includes all the devices belongs to each user which can allow the user to monitor and move between the devices easily.
- **A competitive educational environment:** the system should have the ability to encourage the family members to do better security and gain more knowledge by providing several methods such as quizzes and digital badges and scores.

3.1. Information security policy for home users

In the approach, it is suggested as part of the solution is to use and apply different security policies in order to measure and understand how home users are managing and controlling their security. The need for security policies, processes and procedures becomes more important when there is a need to mitigate internal threats or minimize the possibility of security incidents or threats that can affect information assets and services in organizations (Knapp et al, 2009). Therefore, having security policies with rules, guidelines and measures which can be applicable for home environments can help in managing different security controls and configurations properly which can enhance and improve security practices for home users (Howe et al., 2012; Rao and Pati, 2012; Nthala et al., 2018). Different information security frameworks and well-known standards are used in organisations as a guideline to implement and manage security controls and configurations such as ISO/IEC 27000 series (International Organization for Standardization (ISO), 2013) and NIST Special Publications (NIST, 2019). In addition, several security frameworks and best practices guidelines are offered for small and medium businesses such as the guidelines proposed by The UK National Cyber Security Centre (NCSC, 2018) and IBA (2018). SANS (Thomas, 2001), ITU (2007), US-CERT (2015) and NSA (2016) proposed a range of recommendations and tips for keeping home network secure and helping home users to implement security controls and configurations. All these frameworks, guidelines and best practices are reviewed in order to identify a number of security areas and best practices. Table I presents several security areas with relevant best practices for home network security including but not limited to password security, software security, endpoint protection, data protection and web browsing security, internet connection security and removable media security.

Security Area	Recommended practices
Password Security	Implement strong username and password management
Software Security	Keep system software and applications updated
Internet Connection Security	Use secure internet connections
Endpoint Protection	Install antivirus software
Endpoint Protection	Configure firewall protection
Web browsing Security	Configure web browsers securely
Data Protection	Encrypt data and devices
Data Protection	Enable remote erasure
Software Security	Consider application whitelisting/blacklisting
Software Security	use apps from a trusted source
Data Protection	Back up data
Removable Media Security	Manage and limit the use of removable media such as USB sticks, memory cards, CDs and DVDs.

Table I. Security Best Practices for Home Network and Devices

The official user guide documents for different technologies and devices with different operating systems were reviewed in order to identify the most common security settings and configuration based on the best practice of security for each device, technology and service. Several devices including, but not limited to, computers, laptops, smartphones, tablets, smart TVs and wireless access points are selected and categorized into four different groups as they have similar features and configurations and security controls:

- desktop PCs and laptops group.
- smart phones and tablets group.
- smart TVs and game consoles group.
- wireless access points.

Different groups of security policies such as password policy, software policy, device security policy and internet browser policy are proposed which can contain different security statements in order to monitor and manage different security controls and configurations across different technologies and devices at homes which could help to improve security management and awareness for home users. Each security policy is defined and proposed with three security levels in order to be configured and assigned based on the users' current needs. These security policies act as templates predefined to aid users and save them having to determine dozens of settings and configurations. As an example, Table II presents the statements of the password policy with three suggested security levels which can be applied in desktop and laptop devices.

Category	Policy Statement	Indicative Parameter for The Security Level		
		High	Medium	Low
Password Policy	Password	Enabled	Enabled	Enabled
	Minimum Password Length	12 characters	10 characters	8 characters
	Password Complexity	Enabled	Enabled	Disabled
	Enforce Password History	3 passwords	2 passwords	1 password
	Account lockout duration	30 minutes	15 minutes	Disabled
	Account lockout threshold for Invalid logins	5 Invalid login attempts	10 Invalid login attempts	Disabled
	Time before auto-lock	3 minutes	6 minutes	10 minutes

Table II. The proposed password policy for desktops and laptops

3.2. *The Architecture*

Stemming from the abovementioned requirements, cyber security management and awareness framework is proposed. The proposed system built upon this framework would provide a user-friendly approach based on the user's current needs including a bespoke security awareness that can help in providing better security management and awareness.

In this framework, the administrator is able to monitor and manage different security settings and control in different digital devices within the home environment. In addition, it allows the end-users to check their security compliance with their assigned policies and make them aware of any potential threats or issues. Figure 1 demonstrates the overall architecture of the cyber security management and awareness system.

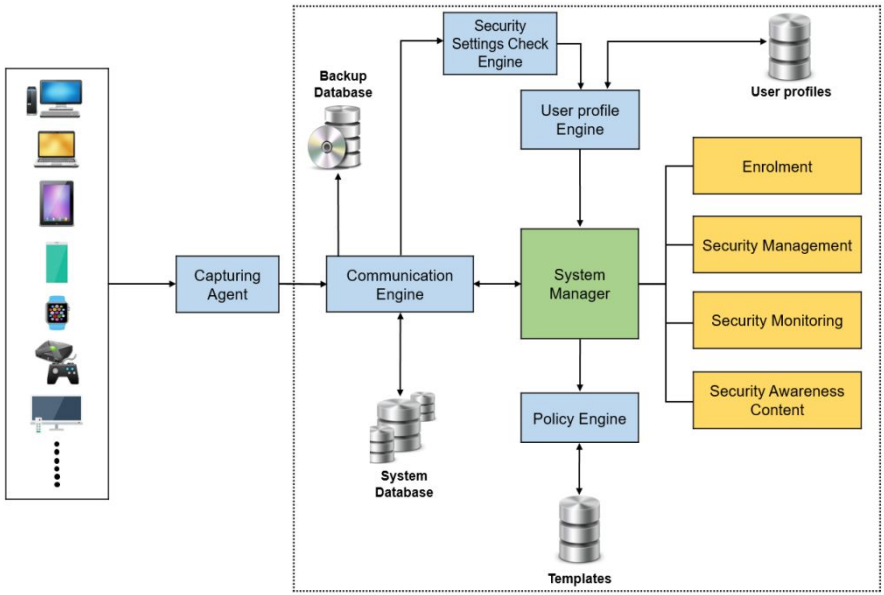

Figure 1. Overall System Architecture

The following sub-sections explain in detail the components required to be used in the architecture in order to fulfil its requirements which can make it more effective, practical and convenient.

3.2.1 *Capturing agent*

The primary role of the Agent is to scan, check, capture the required security information of security controls and settings which are configured in the user's device. In addition, it is responsible for delivering the messages and notification from the system to the users. Due to the variety of technologies, two types of agents are introduced: individual and network-based agents. The individual agent can be installed on the devices such as computers and smartphones. However, there are some IoT devices which are not applicable to install any types of applications such as smart fridge and smart light. A network-based agent can be used to monitor and check the traffic of these devices and get the required information.

The main duty of the agent is to provide communication between the devices and the policy manager, including scan, check, capture the required security information of security

controls and settings which are configured in the user's device. In addition, it is responsible for delivering the messages and notification form the system to the users.

To avoid any security issues or concerns regarding the collection process and the type of security information, the data collected by the agents is general and does not have any confidential information. For example, Table III shows how the required data will be collected, proceeded and stored in the proposed framework.

Security settings/controls	Types of retrieved data	Example
Enabling password	Status	Enabled
Minimum Password Length	The number of characters	8 characters
Password Complexity	Enabled/ disabled	Disabled
Enforce Password History	Number	4 passwords remembered
Antivirus	Status	Enabled
Firewall	Status	Disabled

Table III. An Example of How The System Collects The Required Data

3.2.2 Communication Engine

The main duty of the Communication Engine is to provide communication between the stored data and the main components for the system framework. The data captured by the agents is sent to the Communication Engine in order to be stored securely in the system database. The security information will be retrieved by the Communication Engine to be sent to the Security Settings Check Engine, once the data is stored in the database. In addition, the stored data will be sent to the System Manager via the Communication Engine. Another task performed by the Communication Engine is to enable the System Manager to send the end users some commands (e.g. new enrolment), notifications (e.g. the status) and some awareness contents.

3.2.3 System Manager

The system manager is the main component in the information security management architecture. Its core duty is to enable the user to conduct and achieve a range of different tasks and functions which can be provided by the system. Two different views are offered in the system to the users: administrator and end-users (home users). Nevertheless, the administrator users are given more administrative abilities and duties than end-users. As illustrated in Figure 2, the administrator is granted high-level administrative abilities in order to conduct some administrative tasks. In addition, user's profile can be created, edited and deleted by the administrator. In addition, the administrator can edit and delete the current security policies or add new policies. Moreover, the security awareness contents can be created, reviewed, edited and deleted by the administrator. Furthermore, the administrator can monitor and check the security compliance for the users and devices. On the other hand, the end-users can start the enrolment process for new devices, the request will be pending until it is approved by the administrator. Moreover, the profiles of the managed devices can be viewed by the end-users with the following elements: viewing the policy compliance, viewing the security awareness content, applying an automatic reconfiguration when it is required.

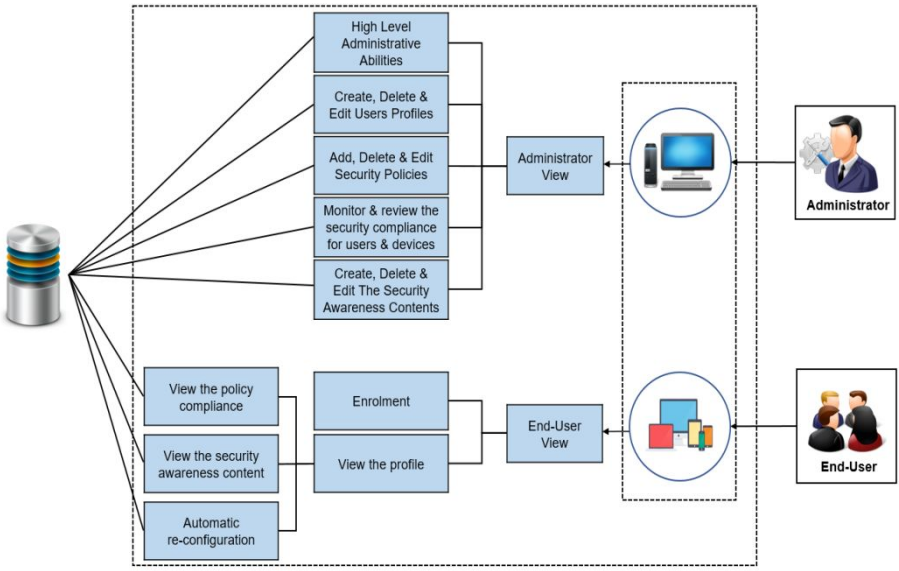

Figure 2. System Manager

3.2.4 Security Settings Check Engine

Once the required information about the security settings is captured by the Capturing Agent and stored in the database via the Communication Engine, the Security Settings Check Engine will review and check the extracted security information and compare it with the assigned policies in order to check whether the device is compliant with the assigned policies or not. Next, the compliance status and the required information will be sent to the user profile. These processes need to be done continuously in order to update the user profile with accurate information. Table IV shows an example of how the settings of the password policy configured in a computer will be compared with the assigned policies in the system in order to check the security compliance.

Password Policy	The device's Configurations	The Assigned Policy	Compliance Status
Password	Enabled	Enabled	✓
Minimum Password Length	8 characters	12 characters	✗
Password Complexity	Disabled	Enabled	✗
Enforce Password History	4 passwords remembered	4 passwords remembered	✓
Account lockout duration	Enabled:10 min	Enabled:10 min	✓
Account lockout threshold for Invalid logins	Disabled	5 Invalid login attempts	✗

Table IV. The Process for Checking The Security Compliance for Password Policy

3.2.5 *The Policy Engine*

The key role of the policy engine is to provide a variety of different security policy templates for different technologies in order to be utilised by the System Manager Engine in order to create a new user profile or update the current one. As discussed previously, several security policies for different devices will be defined and assigned in order to monitor and manage the security configurations for different technologies at homes.

3.2.6 *Information Security Awareness Contents*

As mentioned before that the system is not only proposed to manage the security settings and controls but also to enhance security awareness and knowledge about different threats and issues. The proposed framework tries to raise the user's concern about different types of threats and increase the user's knowledge about different security aspects. In addition, the security awareness messages and contents in the user profile on the client side should be tailored based on the user's knowledge and current needs. The system tries to deliver the awareness contents based on the level of the user's technical experience and the current needs.

3.3. *Mock-up design for the proposed framework*

After presenting a theoretical explanation of the proposed framework used for improving the security management and awareness for home users in the previous section, the next stage of the research focuses on developing a mock-up design that simulates the proposed model. A mockup design has been selected and used for the simulation in the research with interactions applied in many objects in order to enable them to respond to a variety of triggers. Several scenarios were assumed, designed and used during the simulation process for many reasons. First of all, it helps in demonstrating and visualising the real system for managing and monitoring information security for home users. This will allow the main stakeholders to understand the functionalities of the system and how it is supposed to work. In addition, it enables the stakeholders (end-users and experts) to test the usability and functionality early in the development process. Moreover, it helps in acquiring feedback from users about the proposed system.

In the proposed mock-up design, the main menu has been designed to be accessible by the administrator from each section or component. In addition, the visual icon has been utilized in the menu in order to make it easy for the administrator to recognise each component and its task. The proposed mock-up design consists of several components and each component has different tasks: Main Dashboard, Enrolment, Management, Policies, Reports and Support.

3.3.1 *Main dashboard*

The first interface in the proposed design is the main dashboard. The aim of the dashboard is to organise data in a way which makes it easy to understand by the users. This helps to monitor all the home digital devices in a usable and cognitively effective manner. The dashboard is designed to provide information about the home devices such as settings alerts, the status of the enrolled users and their managed devices, statistical information about the status of the devices and their compliance with the assigned policies as shown in Figure 3. The non-compliant settings and devices are coloured in red and compliant settings are coloured in green in order to attract the administrator's attention in a usable method. In addition. Several sections and competent are demonstrated in the dashboard but not limited:

- Security Settings Alert: it shows the current status of several security settings in the managed devices.

- Activity Feed: it displays a list of recent activities performed in the system and the managed devices.
- Security Compliance by Users: it includes the compliance status of all the digital devices owned by each user.
- Security Compliance By Devices: it presents the compliance status for each individual device.
- Security Policies For All The Devices: it shows the compliance of several security policies for all the managed devices.

Figure 3. The main dashboard for administrators

As already mentioned that the proposed tool needs to be usable and flexible in order to be effective and achieve its goals. Therefore, the administrator can have the ability to add new data in a specific section as shown in Figure 4. The selected data can be shown in the sub-window in order to make it easy for the administrator to see how the new data will be presented in the new section.

Figure 4. Adding a New Section in The Dashboard

In addition, Figure 5 shows that the dashboard layout and format can be changed based on the administrator's needs from the settings section in the top menu which can make the system more usable and flexible.

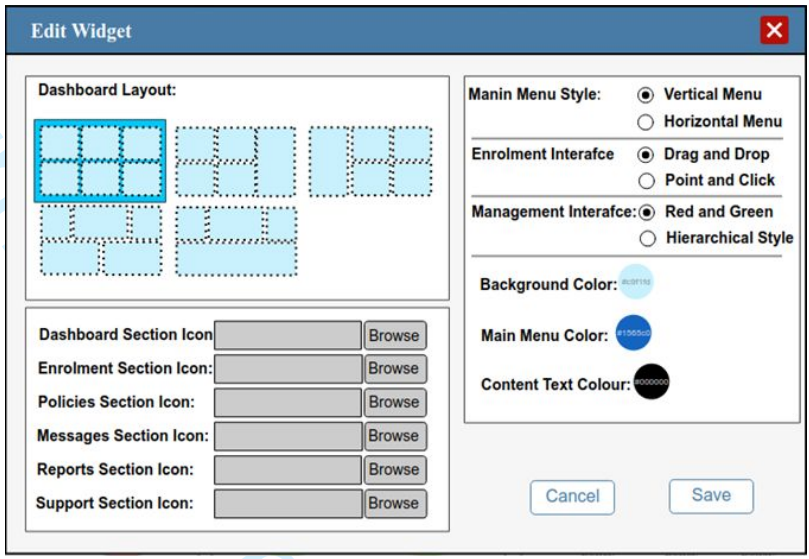

Figure 5. Changing the layout and the format

In addition, the administrator can have the ability to change any section with different data or different styles of presentation as illustrated in Figure 6. This can give the administrator more flexibility to change the data based on his current needs.

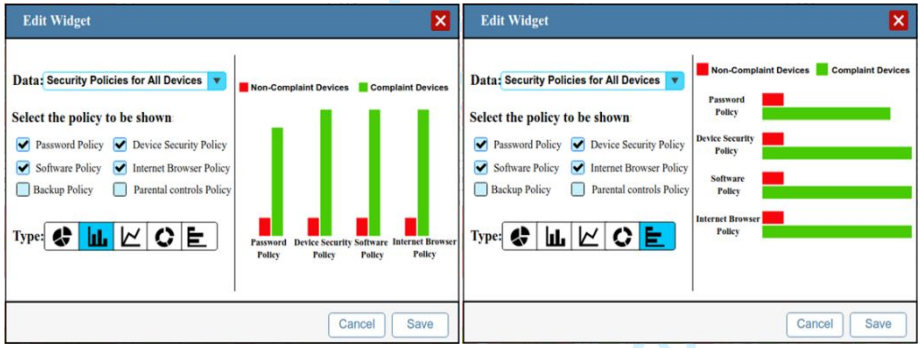

Figure 6. Changing the assigned data or presentation in a section

3.3.2 Device enrolment

The administrator will be notified in the enrolment interface, when there is a new device is descovered by the agents. This can make the system easy to use and effective in establishing the enrolment process. The enrolment processes are designed based on the user's technical experience in order to avoid any difficulty and to add more granularity into the system. For example, most of the enrolment processes for novice users are done automatically as they do not have the appropriate skills to get enrolled properly. Figure 7 shows the enrolment process for novice users.

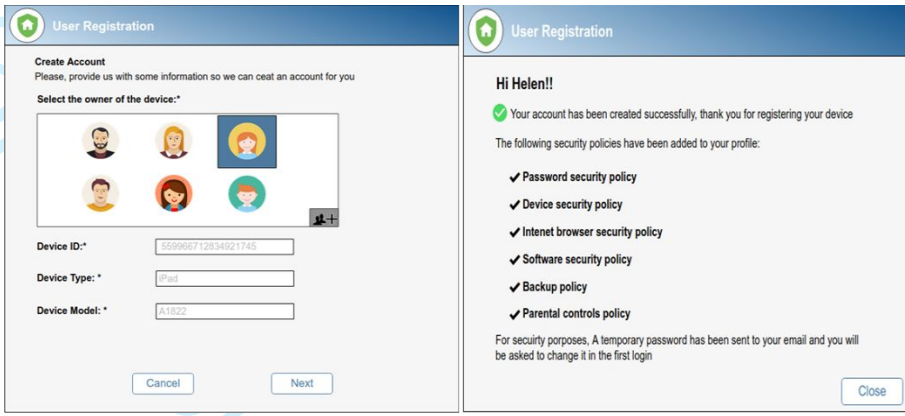

Figure 7. The enrolment process for novice users

It is expected that the intermediate and expert users have good security knowledge and skills as it was shown in the survey's result. Therefore, they can be provided in the system with an option to choose the required security policies and the level based on the current needs as shown in Figure 8.

Figure 8. The enrolment process for intermediate and expert users

3.3.3 Management Interface

The management section is responsible for managing, monitoring and checking the compliance of the enrolled devices with their assigned policies. The interface is designed as a hierarchical style which can give a panoramic view of all the managed users and their enrolled devices. In addition, Red and green colours are utilised to illustrate the non-compliant and compliant devices in order to facilitate administrative tasks. In addition, the administrator can view all the users together by selecting "All" or a specific user can be only displayed by clicking on the specific name and the rest of the users will be blurred as shown in Figure 9. All these features can make the system easier and more flexible.

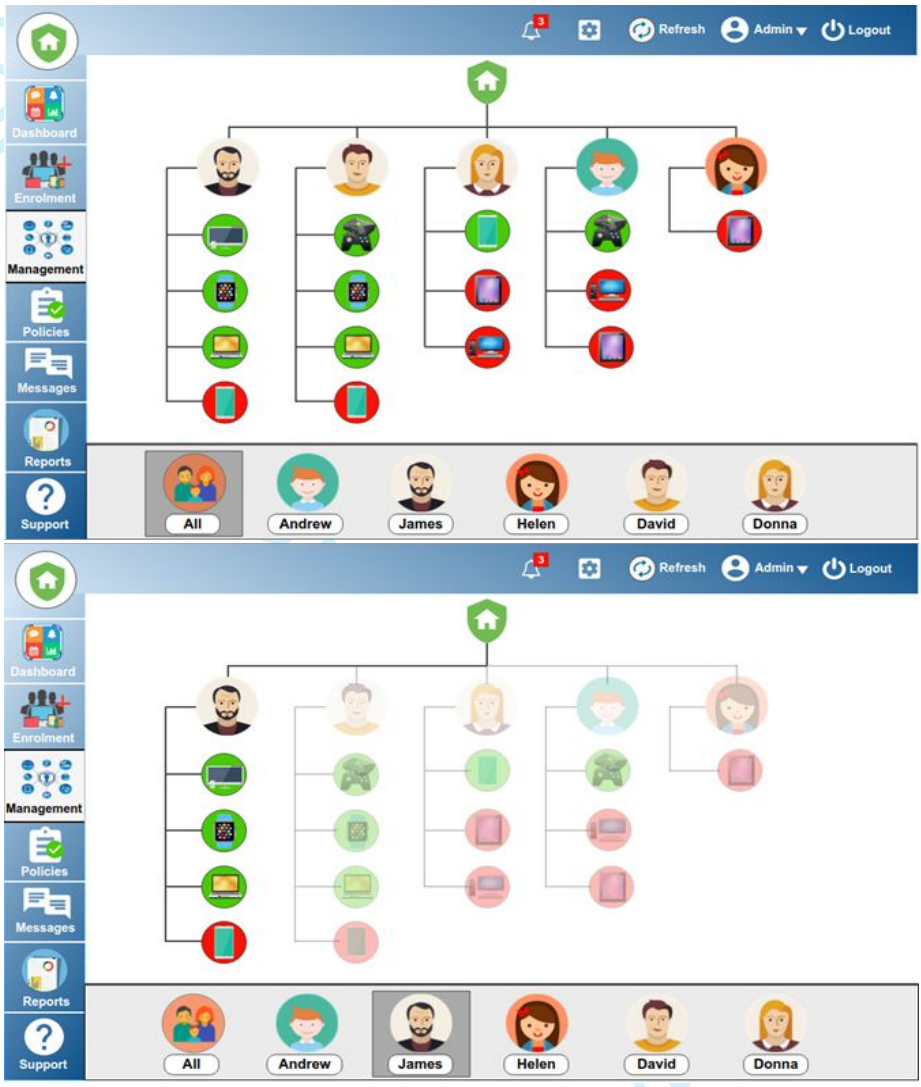

Figure 9. The management interface for the enrolled users

As illustrated in Figure 10, A description box can be displayed when the administrator does a mouseover on a specific device, which provides some information about the device. The box border is coloured in green or red in order to attract the administrator's attention. In addition, this can make the management procedures and processes are easy and convenient for them. In addition, more options can be provided to the administrator such as viewing profiles, changing the owner, sending messages to the users and removing the devices. This can add a good enhancement in managing the tool effectively make the process of the management easy for administrators.

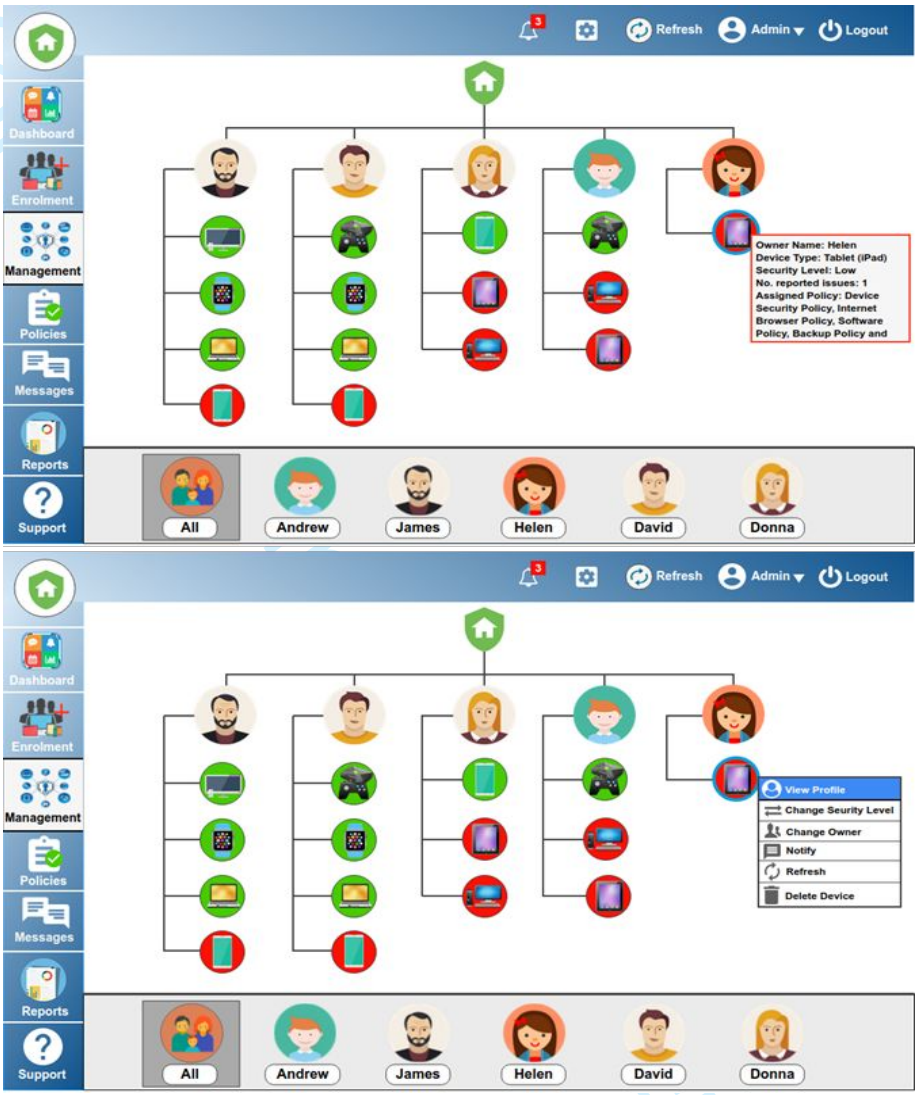

Figure 10. Mouseover and Right-Click option in the management interface

The administrator is provided with a comprehensive profile for the selected user which can show the device compliance in a usable way as shown in Figure 11. The policies are designed as a horizontal clickable menu with a green tick and a red cross icon to show the status of the compliance. In addition, the profile includes a recent activity section, a profile summary and the current alerts. Moreover, changing the current owner or the security level can be done via the interface. The whole layout of the profile or a specific section can be changed and customised based upon the administrator's priority in order to achieve the system's goals. In addition, a top menu in the profile is provided for administrators in order to navigate and move easily between the devices owned by one user.

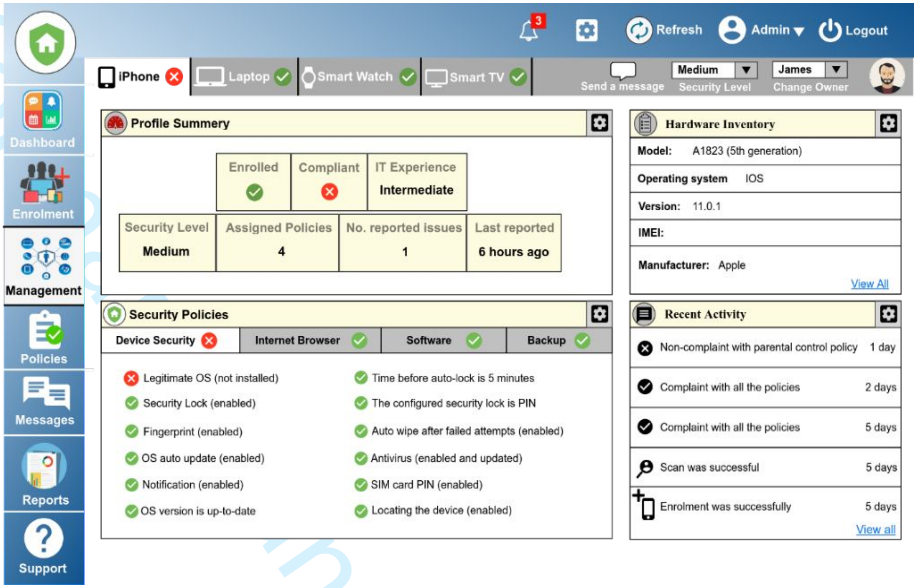

Figure 11. The user profile for a specific user

3.3.4 Policy Interface

The administrator is provided with a submenu which allows him to view, edit and delete any policy from the current policies in the system or add a new policy. This can help administrators in managing the security policies in the system easily. Once the administrator selects a specific policy, and click the view button, the whole sub-policies will be shown as illustrated in Figure 12. In addition, the administrator can select a security level to view the configured settings for the selected policies. Moreover, the administrator can get more explanation about each policy statement by clicking on the red information icon beside each statement. The administrator can easily move between the policies by clicking on each one in order to expand and show the policy statements. All these options and features can make the process of managing security policies in the system usable and fixable.

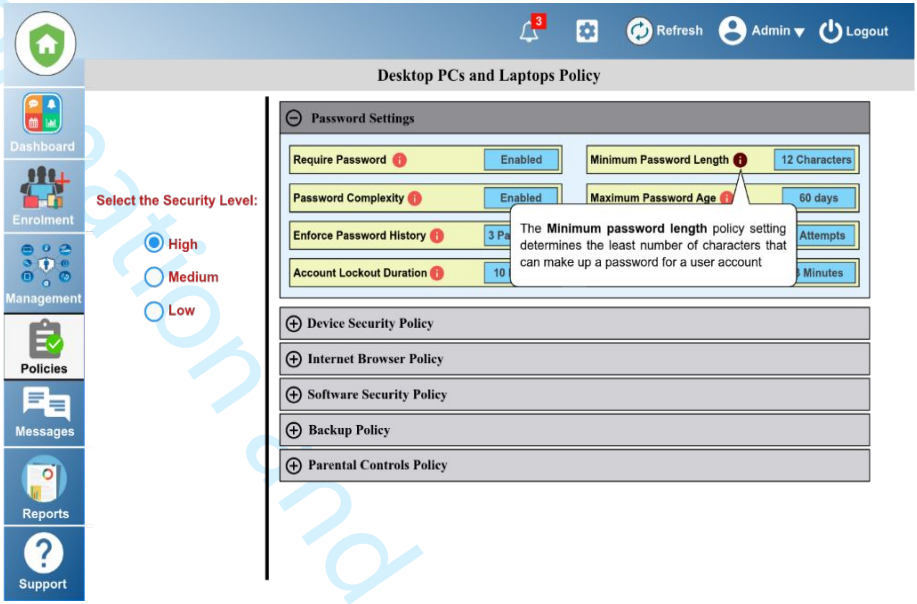

Figure 12. Security policies for desktop and laptop devices

3.3.5 User profile (For End User)

Each user is provided with a user profile which contains information about the security status and the assigned policies for each device. The layout of the interface and the added sections can be changed by the user from the setting section. The user profile is designed to notify the user and make them aware of the current issues or potential threats by providing the users with several sections such as the profile summary, recent activity and policy compliance. In addition, the profile aims to enhance cyber security knowledge and awareness for home users. Therefore, Do You Know section provides some statistical incidents which can raise the user's concern in order to enhance the level of security knowledge and manage the security controls effectively. In addition, Quiz section can be provided to increase the user's security knowledge. It can be seen in Figure 13 that the user is intermediate and he has one issue in a security policy that he does not have antivirus protection. As a result, the provided information in Do You Know section and the Quizz all is about the importance of antivirus and the virus threats.

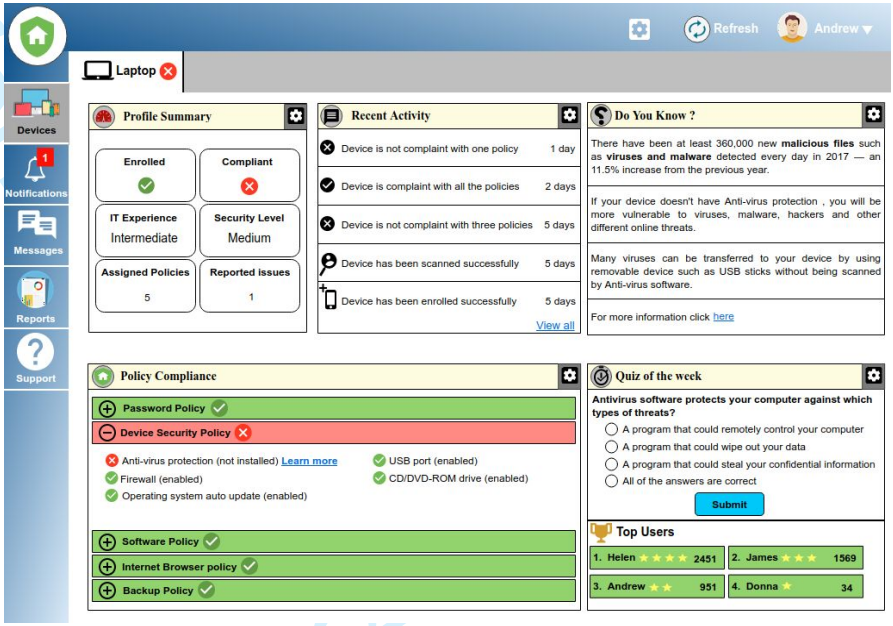

Figure 13. User Profile for Intermediate user

On the other hand, if a novice user has an issue in one security policy, Do You Know section and the Quiz section will provide information about different security aspects in order to raise the security concern and knowledge. As shown in Figure 14, the user has an illegitimate OS but the two sections still give information and knowledge about many aspects.

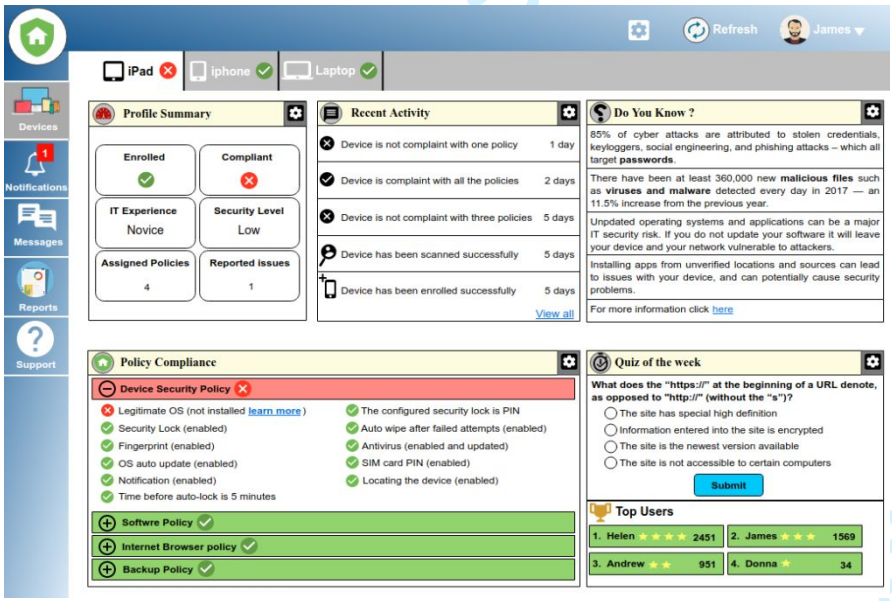

Figure 14. The user profile for a novice user

Users are provided with a link beside each policy statement which has an issue. This link offers the user a window that has more information about the current issue as illustrated in Figure 15. Only the novice users are provided with a quick troubleshoot for the current possible threat by doing automatic reconfiguration or installation on behalf of the users who do not have good technical knowledge. In addition, more tips and advice about the current risk is offered in the same window. Another option can be provided for users is Ask Community option. It is a collaborative website which allows the home users to share their knowledge, experience and advice about a variety of security issues and threats. This can increase the learnability and allow users to gain more knowledge about securing their devices and networks.

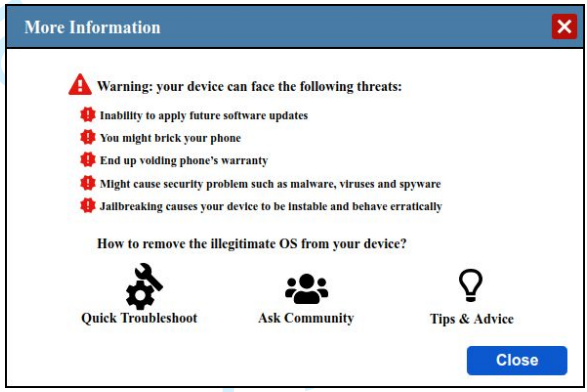

Figure 15. More information for novice users

4 Evaluation of the proposed approach

After designing a simulated design for the proposed approach, a qualitative evaluation (focus group) was carried out. The aim of the focus group method is to evaluate the validation and usability aspect and gain feedback from experts about the proposed approach for improving cyber security management and awareness for home users. The experts were recruited for the focus group discussion at The Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), July 2019, in Nicosia. The invitations and the selection process have been facilitated by the conference organisers. Initially, 5 participants were invited to the session. However, one participant left the session as he had an urgent duty. 14 open-ended qualitative questions were selected and designed for the focus group session. The questions were drafted and reviewed in terms of being understandable and objective in order to enrich the discussion and gain more feedback and comments from the participants in order to achieve the aims of the focus group session.

A live demonstration for the proposed system with different scenarios was conducted at the beginning of the focus group session. In addition, information sheets and consent forms were provided to give them more information about the research study. Moreover, the participants were informed that their participation is voluntary and their personal information will be kept anonymous and confidential.

In general, all the interviewed experts agreed that the problem which is identified by the research is very important and valid as many online devices are being used in homes without monitoring, managing and configuring them with the appropriate security controls and settings.

Most of the experts felt that the proposed approach is feasible and possible at the operation level. On expert mentioned that the approach is feasible to be a workable solution in a real environment but monitoring and managing security configuration and controls in some of the IoT devices might be a hard task as these devices have different operating systems, configurations and services.

The utilisation of the security policies in the proposed approach, the participants agreed that the idea of using a number of security policies in the proposed approach is useful and effective in providing good security management for different devices, applications and platforms. One expert stated that "the security policy is already used widely in organisations and I think if it can be applied for home users with some changes, it would be very useful and effective in managing the security settings and configurations in home devices". In addition, they argued that it is a good idea to allow the proposed system to provide novice users with a minimum level of security requirements (low level) which needs to be implemented in their devices. However, two participants did not like the idea of providing three different security levels for home users, they suggested that the policy settings can be modified by the administrator for the users without providing different security levels.

Usefulness of the proposed approach, it is important to investigate the benefit that home users might gain by implementing the proposed approach. The participants generally agreed that the proposed approach would be useful for home users. They indicated that it would succeed in providing better security monitoring, security management and awareness in home environments. One expert stated that "in my opinion, if the proposed tool is implemented in a real environment, it would enhance the security management and awareness for home users."

The success of the proposed design in validating the approach, the experts felt that the proposed design has provided a robust validation of the approach. They indicated that the proposed design was beneficial enough to visualise the main concept and components of the proposed approach. On expert said: "apart from the technical aspects, I think the proposed design has succeeded in showing how the system would work in the real environment by interacting with different components and sections".

The strength of the proposed approach and design, most of the participants agreed that applying different security policies in the proposed approach is a very good idea which can cover different security aspects in different devices. All the participants indicated that that proposed design has good usable interfaces with applying different functions and colours, especially Red and Green. On experts stated that "I think the idea of using Red and Green is very useful to let administrators or users recognise the current issues easily". Two experts said that the approach is not only a management tool but also provides the users with some tips, advice and quizzes, which can improve the users' knowledge and skills effectively.

The usability and convenience of the interfaces and design, the respondents generally agreed the proposed design is usable and convenient. They argued that that the main dashboard interface is usable and effective and it provides the administrators with the required information. In addition, they argued that the enrolment process implemented in the proposed approach is effective and flexible as different procedures are provided for the users based on their technical skills and knowledge. Moreover, they agreed that the management interface and the user profile is usable and provide the required information for the administrators which can help them in recognising the current issues or threats easily and managing digital devices effectively.

As regards weaknesses, some of the participants argued that one of the barriers in the proposed approach is how to persuade home users and family members to use the proposed approach when it is implemented in real homes. On expert stated that "In my opinion, the

main barrier is how you will get people and convince them to use this system". Another barrier mentioned by one participant is that more work needs to be done on how the settings in different devices and operating system will be collected and checked. In addition, the same participant had another concern about the person who will be assigned as an administrator to manage the proposed tool in a novice family.

5 Conclusion and future research

The main objective of this research was to define and propose a novel approach that can help in enhancing security management and awareness for home users in a usable manner. This objective was achieved by investigating the current state of the art and related works to identify the gap as regards the information security management and awareness for home users. From the perspective of the authors, the proposed framework can assist home users to monitor and manage security settings and controls of digital devices. In addition, it can help in educating home users and provide them with tailored security awareness based on their current needs. These goals can be achieved by applying different groups of security policies which can manage many security controls and configurations in several digital devices.

Thus, a novel framework was designed and a mock-up design was developed to simulate to simulate the proposed approach using with different scenarios to validate the defined approach. The proposed approach and the mock-up design were evaluated by experts within the domain of the research. The overall feedback of the two discussions about the research and the proposed approach and design was positive and promising. In addition, several recommendations and limitations were raised and discussed in order to be improved in further research work. On the other hand, a complete prototype system needs to be developed for the proposed system in a real environment within the home network. This will be useful in order to understand the efficiency of the proposed approach in monitoring and managing the security controls and settings which will result in improving the security management and awareness for home users. In addition, implementing the system in a production environment will help in evaluating the system effectively and discover any limitations.

References

Alotaibi, F., Clarke, N. and Furnell, S. (2017) 'An Analysis of Home User Security Awareness & Education', in *2017 12Th International Conference for Internet Technology and Secured Transactions (Icitst)*. Cambridge, pp. 116–122. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8356359&isnumber=8356324.

Alotaibi, F., Clarke, N. L. and Furnell, S. (2019) 'Holistic Information Security Management for Home Environments', in Furnell, S. and Clarke, N. L. (eds) *Thirteenth International Symposium on Human Aspects of Information Security & Assurance, {HAISA} 2019, Nicosia, Cyprus, July 15-16, 2019, Proceedings*. University of Plymouth, pp. 20–33. Available at: https://www.cscan.org/?page=openaccess&eid=21&id=399.

Furnell, S. M., Bryant, P. and Phippen, a. D. (2007) 'Assessing the security perceptions of personal Internet users', *Computers and Security*, 26(5), pp. 410–417.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M. and Byrne, Z. (2012) 'The Psychology of Security for the Home Computer User', in *2012 IEEE Symposium on Security and Privacy*. San Francisco, pp. 209–223.

IBA (2018) *Cybersecurity Guidelines Cyber Security Guidelines By the IBA's Presidential Task Force on Cyber Security*. Available at: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (Accessed: 27 October 2019).

International Organization for Standardization (ISO) (2013) *ISO/IEC27002: 2013 Information technology—Code of practice for information security controls*, *Iec*.

ITU (2007) *ITU-T Recommendation X.1111: Framework of security technologies for home network*, *International Telecommunication Union*. Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1111-200702-I!!PDF-E&type=items.

Jahankhani, H., Jayaraveendran, T. and Kapuku-Bwabw, W. (2011) 'Improved awareness on fake websites and detecting techniques', in *Global Security, Safety and Sustainability & e-Democracy*. Berlin, Heidelberg: Springer, pp. 271–279.

Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers and Security*. Elsevier Ltd, 29(8), pp. 840–847. Available at: http://dx.doi.org/10.1016/j.cose.2010.08.001.

Kritzinger, E. and Von Solms, S. H. (2013) 'Home User Security- from Thick Security-oriented Home Users to Thin Security- oriented Home Users', *Science and Information Conference (SAI), 2013*, pp. 340–345. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6661760.

Labuschagne, W. A. and Eloff, M. (2012) 'Towards an automated security awareness system in a virtualized environment', in *11th European Conference on Information Warfare and Security*. Laval: Academic Conferences International Limited., pp. 163–171.

LaRose, R., Rifon, N. J. N. and Enbody, R. (2008) 'Promoting personal responsibility for internet safety', *Communications of the ACM*, 51(3), pp. 71–76.

Lunsford, P. and Boahn, C. (2015) *How the Lizard Squad Took Down Two of the Biggest Networks in the World*. Available at: https://infosecwriters.com/Papers/JRollins_Lizard_Squad.pdf (Accessed: 1 March 2019).

Magaya, R. T. and Clarke, N. L. (2012) 'Web-based risk analysis for home users', in *10th Australian Information Security Management Conference, AISM 2012*, pp. 19–27.

Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017) 'A survey of distributed denial-of-service attack, prevention, and mitigation techniques', *International Journal of Distributed Sensor Networks*, 13(12).

Maurer, M., Luca, A. De and Kempe, S. (2011) 'Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness', in *the Seventh Symposium on Usable Privacy and Security*, p. 2.

National Office of Statisitcs (2018) *Internet access - households and individuals, Great Britain: 2018*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (Accessed: 2 March 2019).

NCSA and PayPal (2013) *2013 NATIONAL ONLINE SAFETY STUDY*. Available at: https://staysafeonline.org/download/datasets/7358/2013 NCSA Online Safety Study.pdf (Accessed: 22 June 2017).

NCSC (2018) *10 steps to cyber security - NCSC*. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps (Accessed: 25 October 2019).

Ng, B. B.-Y. and Rahim, M. A. (2005) 'A Socio-Behavioral Study of Home Computer Users ' Intention to Practice Security', *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 2003, pp. 234–247. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=pacis2005.

NIST (2019) *NIST Publications*. Available at: https://csrc.nist.gov/publications (Accessed: 21 October 2019).

Nouh, M. *et al.* (2014) 'Social Information Leakage: Effects of Awareness and Peer Pressure on User Behavior', in Tryfonas, T. and Askoxylakis, I. (eds) *Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer International Publishing, pp. 352–360.

NSA (2016) *Best Practices for Keeping Your Home Network Secure*. Available at: https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf (Accessed: 14 October 2019).

Nthala, N., Flechais, I., Nthala, N. and Flechais, I. (2018) 'Informal Support Networks : an investigation into Home Data Security Practices', *In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pp. 63–82.

Rao, U. H. and Pati, B. P. (2012) 'Study of internet security threats among home users', in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*. Sao Carlos, pp. 217–221. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6412405.

Reynolds, M. (2016) *TalkTalk and Post Office customers hit by Mirai worm attack*. Available at: https://www.wired.co.uk/article/deutsche-telekom-cyber-attack-mirai (Accessed: 19 March 2019).

Sharifi, M., Fink, E. and Carbonell, J. G. (2011) 'SmartNotes: Application of crowdsourcing to the detection of web threats', *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, pp. 1346–1350.

Smith, A., Papadaki, M. and Furnell, S. M. (2013) 'Improving awareness of social engineering attacks', *IFIP Advances in Information and Communication Technology*, 406, pp. 249–256.

Statista (2019) *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. Available at: www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. (Accessed: 5 April 2019).

Thomas, K. (2001) *Building a Secure Home Network*, *SANS Institute*.

Tolnai, A. and Von Solms, S. (2009) 'Solving security issues using information security awareness portal', *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, pp. 1–5.

US-CERT (2015) *Security Tip (ST15-002): Home Network Security*, *NCCIC Publications*. Available at: https://www.us-cert.gov/ncas/tips/ST15-002 (Accessed: 14 October 2019).

Volkamer, M., Renaud, K., Canova, G., Reinheimer, B. and Braun, K. (2015) 'Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness', in *International Conference on Trust and Trustworthy Computing, TRUST 2015,*. Cham: Springer, pp. 104–122.

Watson, B. and Zheng, J. (2017) 'On the User Awareness of Mobile Security Recommendations', *Proceedings of the SouthEast Conference*, (ACM), pp. 120–127.

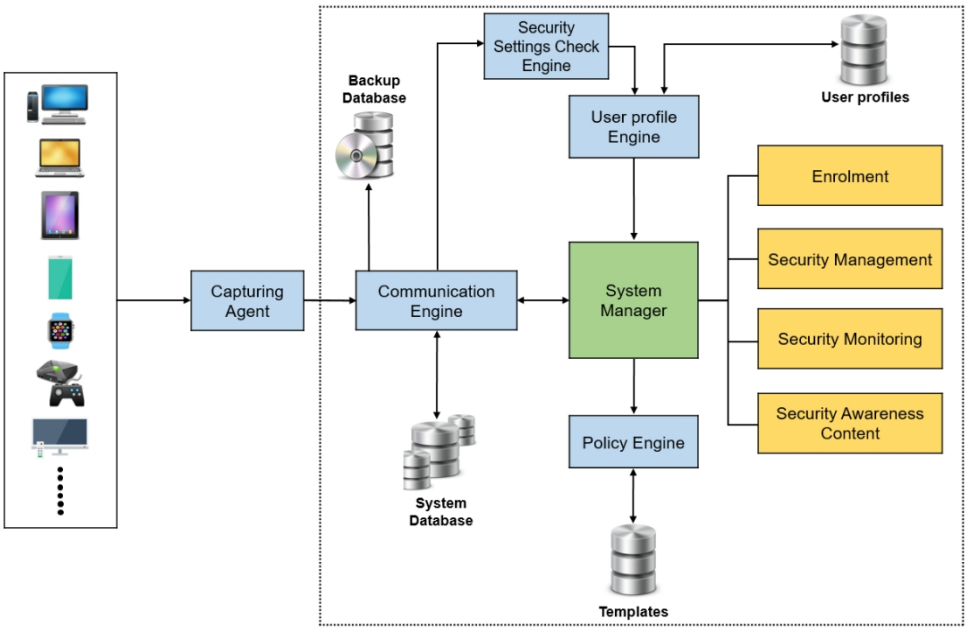

Figure 1. Overall System Architecture

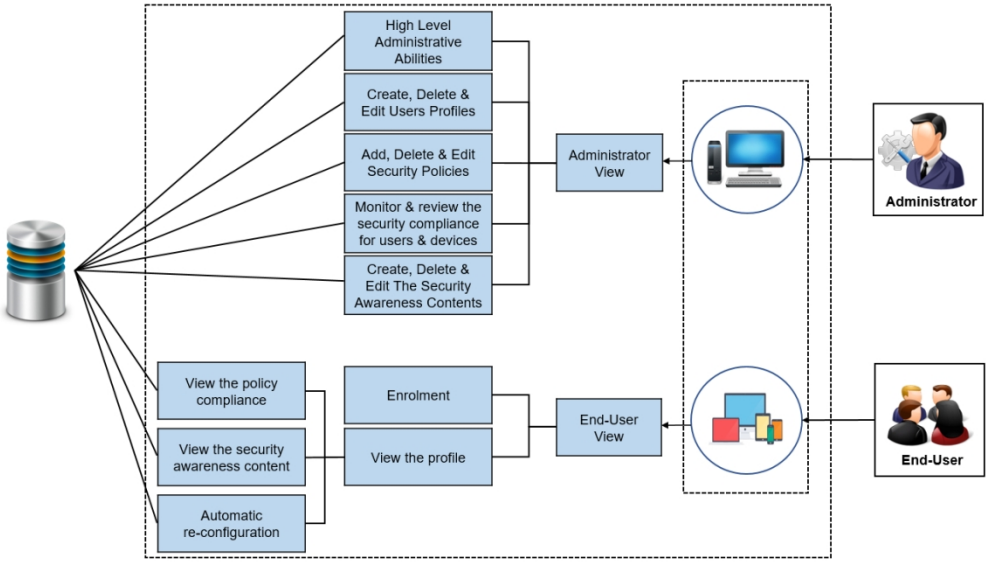

Figure 2. System Manager

Figure 3. The main dashboard for administrators

Figure 4. Adding a New Section in The Dashboard

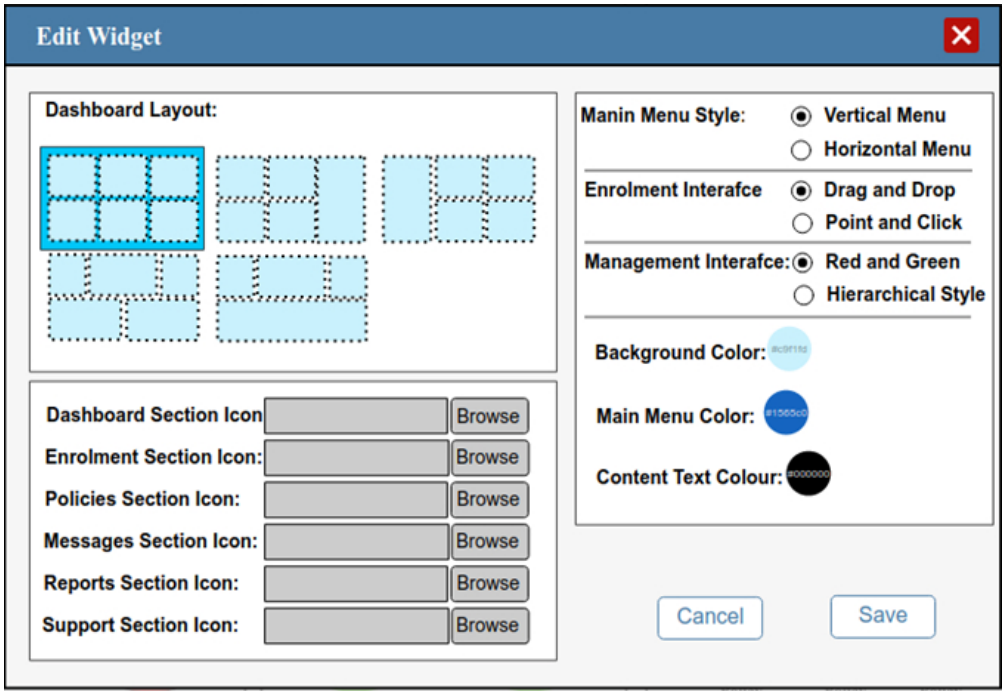

Figure 5. Changing the layout and the format

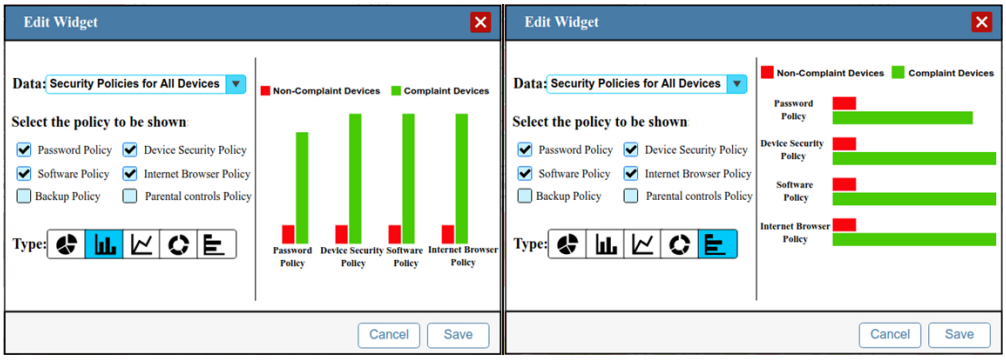

Figure 6. Changing the assigned data or presentation in a section

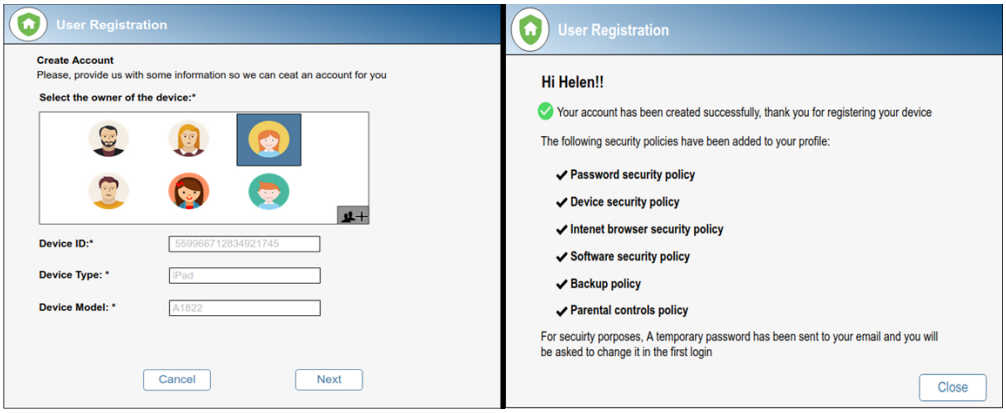

Figure 7. The enrolment process for novice users

Figure 8. The enrolment process for intermediate and expert users

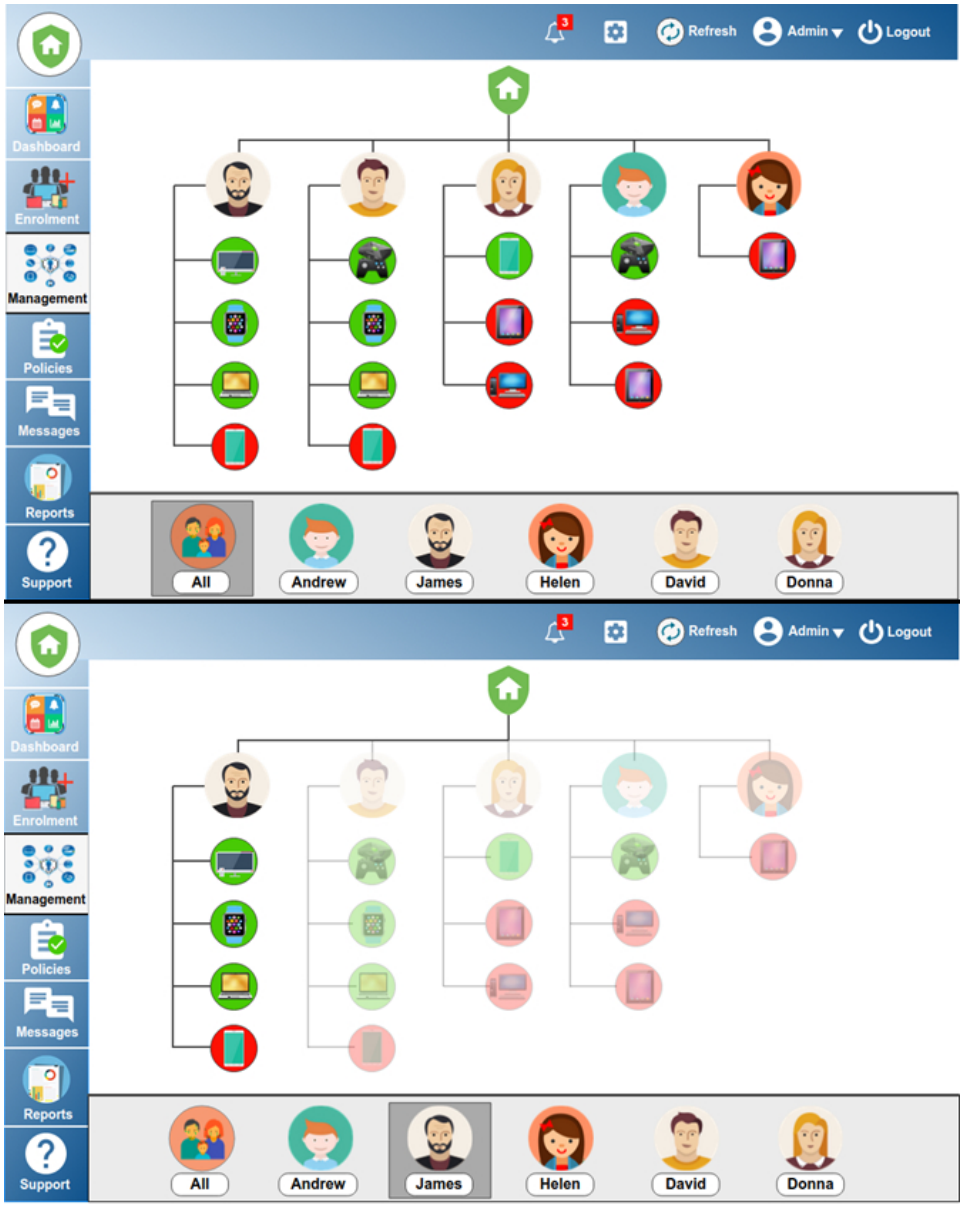

Figure 9. The management interface for the enrolled users

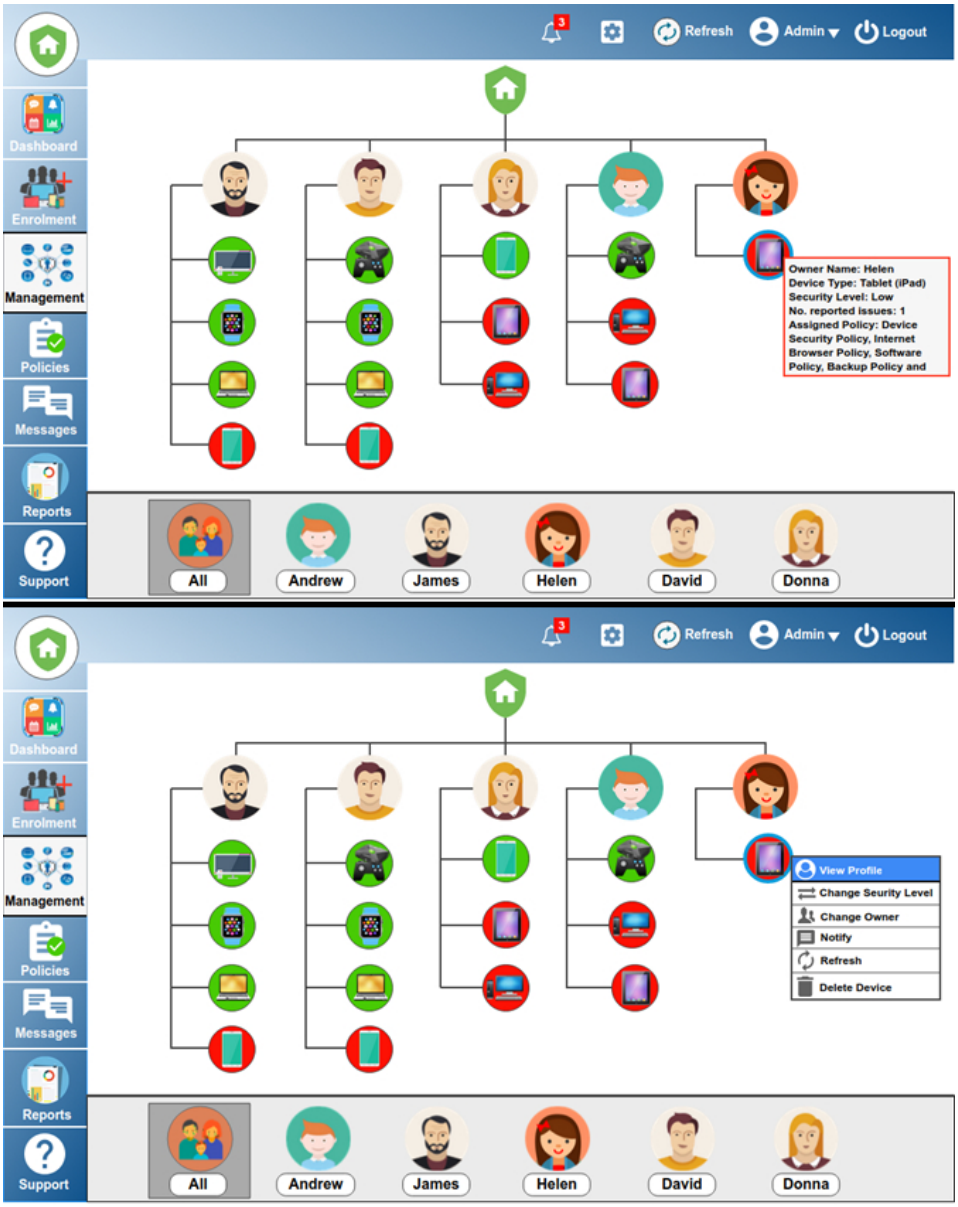

Figure 10. Mouseover and Right-Click option in the management interface

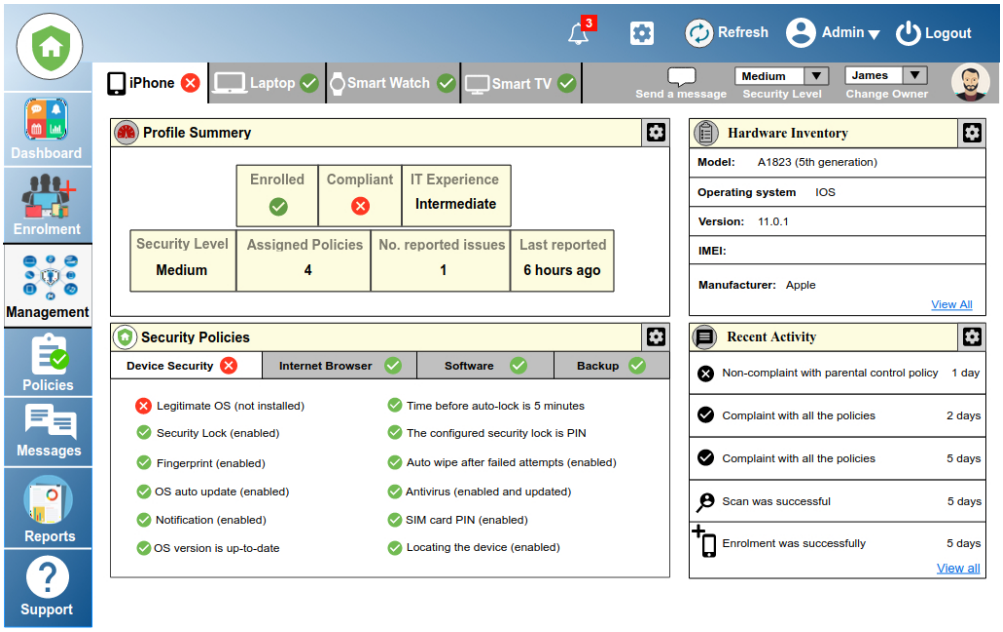

Figure 11. The user profile for a specific user

361x226mm (72 x 72 DPI)

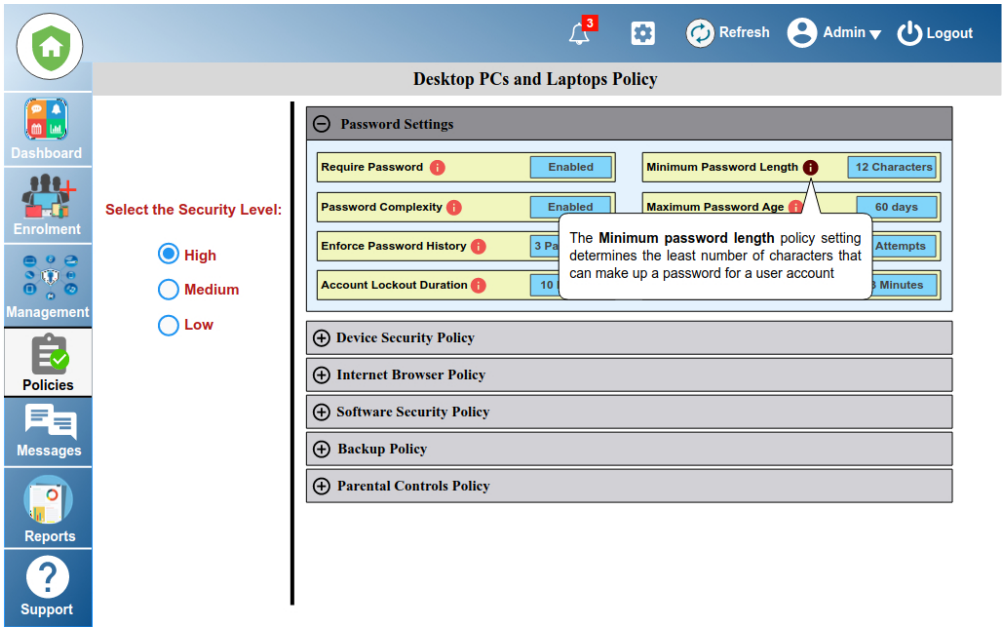

Figure 12. Security policies for desktop and laptop devices

361x225mm (72 x 72 DPI)

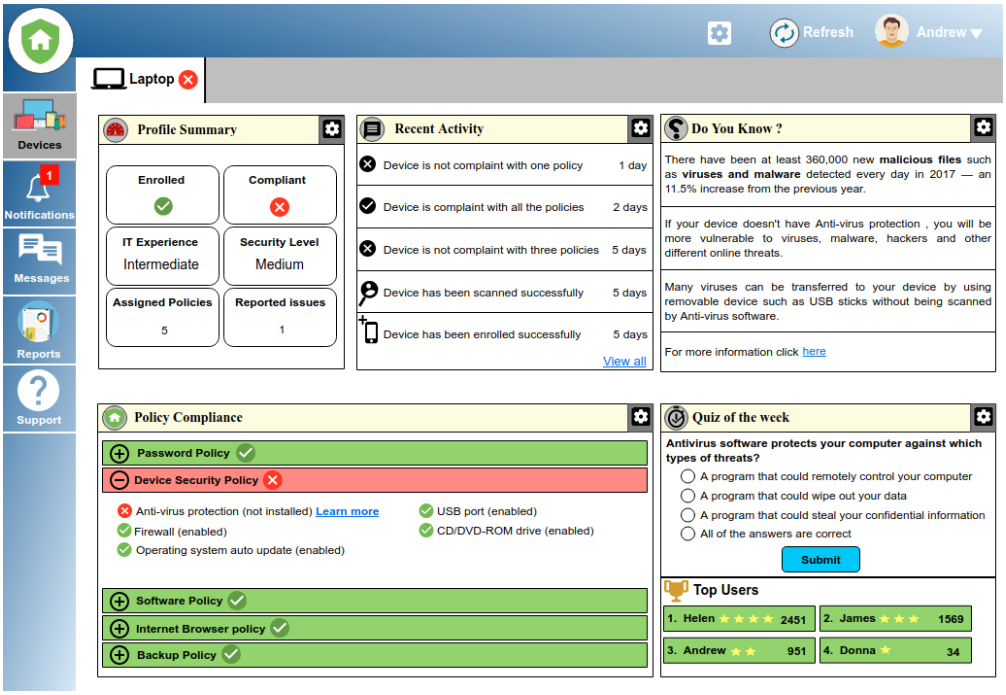

Figure 13. User Profile for Intermediate user

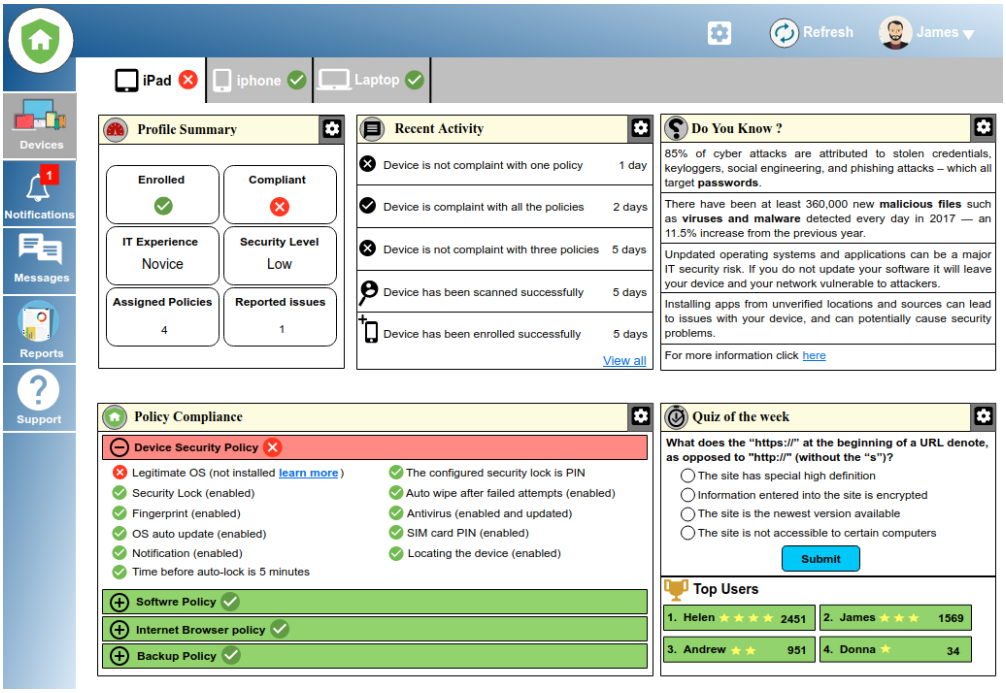

Figure 14. The user profile for a novice user

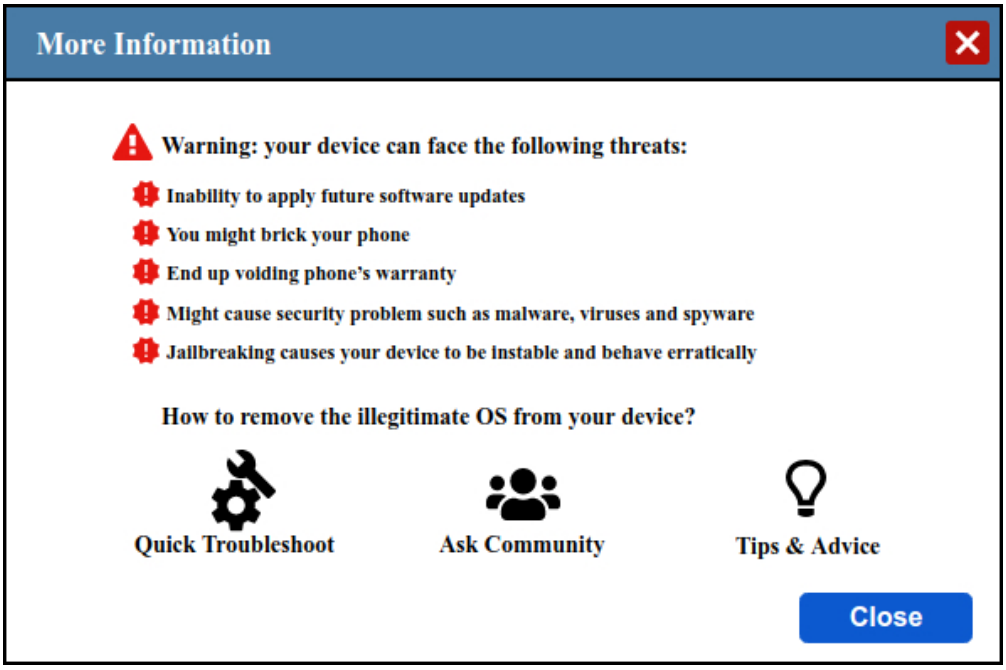

Figure 15. More information for novice users

Security Area	Recommended practices
Password Security	Implement strong username and password management
Software Security	Keep system software and applications updated
Internet Connection Security	Use secure internet connections
Endpoint Protection	Install antivirus software
Endpoint Protection	Configure firewall protection
Web browsing Security	Configure web browsers securely
Data Protection	Encrypt data and devices
Data Protection	Enable remote erasure
Software Security	Consider application whitelisting/blacklisting
Software Security	use apps from a trusted source
Data Protection	Back up data
Removable Media Security	Manage and limit the use of removable media such as USB sticks, memory cards, CDs and DVDs.

Table I. Security Best Practices for Home Network and Devices

Security Area	Recommended practices
Password Security	Implement strong username and password management
Software Security	Keep system software and applications updated
Internet Connection Security	Use secure internet connections
Endpoint Protection	Install antivirus software
Endpoint Protection	Configure firewall protection
Web browsing Security	Configure web browsers securely
Data Protection	Encrypt data and devices
Data Protection	Enable remote erasure
Software Security	Consider application whitelisting/blacklisting
Software Security	use apps from a trusted source
Data Protection	Back up data
Removable Media Security	Manage and limit the use of removable media such as USB sticks, memory cards, CDs and DVDs.

Category	Policy Statement	Indicative Parameter for The Security Level		
		High	Medium	Low
Password Policy	Password	Enabled	Enabled	Enabled
	Minimum Password Length	12 characters	10 characters	8 characters
	Password Complexity	Enabled	Enabled	Disabled
	Enforce Password History	3 passwords	2 passwords	1 password
	Account lockout duration	30 minutes	15 minutes	Disabled
	Account lockout threshold for Invalid logins	5 Invalid login attempts	10 Invalid login attempts	Disabled
	Time before auto-lock	3 minutes	6 minutes	10 minutes

Table II. The proposed password policy for desktops and laptops

Category	Policy Statement	Indicative Parameter for The Security Level		
		High	Medium	Low
Password Policy	Password	Enabled	Enabled	Enabled
	Minimum Password Length	12 characters	10 characters	8 characters
	Password Complexity	Enabled	Enabled	Disabled
	Enforce Password History	3 passwords	2 passwords	1 password
	Account lockout duration	30 minutes	15 minutes	Disabled
	Account lockout threshold for Invalid logins	5 Invalid login attempts	10 Invalid login attempts	Disabled
	Time before auto-lock	3 minutes	6 minutes	10 minutes

Security settings/controls	Types of retrieved data	Example
Enabling password	Status	Enabled
Minimum Password Length	The number of characters	8 characters
Password Complexity	Enabled/ disabled	Disabled
Enforce Password History	Number	4 passwords remembered
Antivirus	Status	Enabled
Firewall	Status	Disabled

Table III. An Example of How The System Collects The Required Data

Security settings/controls	Types of retrieved data	Example
Enabling password	Status	Enabled
Minimum Password Length	The number of characters	8 characters
Password Complexity	Enabled/ disabled	Disabled
Enforce Password History	Number	4 passwords remembered
Antivirus	Status	Enabled
Firewall	Status	Disabled

Password Policy	The device's Configurations	The Assigned Policy	Compliance Status
Password	Enabled	Enabled	✓
Minimum Password Length	8 characters	12 characters	✗
Password Complexity	Disabled	Enabled	✗
Enforce Password History	4 passwords remembered	4 passwords remembered	✓
Account lockout duration	Enabled:10 min	Enabled:10 min	✓
Account lockout threshold for Invalid logins	Disabled	5 Invalid login attempts	✗

Table IV. The Process for Checking The Security Compliance for Password Policy

Password Policy	The device's Configurations	The Assigned Policy	Compliance Status
Password	Enabled	Enabled	✓
Minimum Password Length	8 characters	12 characters	✗
Password Complexity	Disabled	Enabled	✗
Enforce Password History	4 passwords remembered	4 passwords remembered	✓
Account lockout duration	Enabled:10 min	Enabled:10 min	✓
Account lockout threshold for Invalid logins	Disabled	5 Invalid login attempts	✗